

I. General Remarks Concerning This Response

Claims 1-30 are currently pending in the present application. No claims have been amended, added, or canceled. Reconsideration of the claims is requested.

II. Summary of Present Invention

A method and system are presented for managing access to resources with a role-based access control model that includes dynamic update functionality using role filters and capability filters, also termed "active roles". Rather than having a security administrator specifically connect individual users to a role, a role filter is defined for a role. The role filter is evaluated to determine which users should be matched to a given role, and matching users are then automatically associated with the given role. Using role filters, one can create business rules for role-based resource access based on employee title, organization, job status, or project assignment.

In addition to its role filter, each named role contains a set of access capabilities. Each capability contains a set of access conditions and a capability filter. Each access condition has a set of rights and any qualifications or conditions to those rights. Similar to the operation of a role filter, capability filters can be used to describe the set of instances to which a particular capability should apply. Rather than having a security administrator specifically connect individual resources to a capability, the administrator can define a capability filter for each capability. As target instances are added, deleted, or changed, capability filters are re-evaluated to maintain the appropriate set of relationships.

III. 35 U.S.C. § 102(b)-Anticipation-Bapat et al.

The Office action has rejected claims 1-30 under 35 U.S.C. § 102(b) as anticipated by Bapat et al., "System and method for restricting database access to managed object information using a permissions table that specifies access rights corresponding to user access rights to the managed objects", U.S. Patent No. 6,038,563, filed 03/25/1998, issued 03/14/2000. This rejection is respectfully traversed.

The rejection of independent claim 1 states in its entirety:

As per the following claims, Bapat discloses:

1. A method for controlling access rights of a requesting principal to a protected resource in a computer system, wherein a principal is associated with at least one role, the method comprising:

- associating a role filter with a role (column 10);
- associating a set of one or more capabilities with the role (column 10);
- associating a capability filter with a capability in the set of one or more capabilities (column 10); and
- authorizing access for the requesting principal to the protected resource based on an association between the requesting principal and the role and based on an association between the protected resource and a capability of the role (columns 11-12).

As is apparent from the copy of the rejection that is included hereinabove, the rejection does not provide any detail or any argument as to which elements of the system that is disclosed in Bapat et al. correspond to the claimed elements of the present application. The rejection merely points to an entire column of text within Bapat et al. for the first three claim elements and then points to two entire columns of text within Bapat et al. for the fourth claim element. Applicant asserts that the lack of explanatory detail in the rejection with respect to individual claim elements mirrors the lack of disclosure in Bapat et al. with respect to the claimed features. In other words, the rejection points to entire sections of Bapat et al. rather than comparing specific features of Bapat et al. against specific claim elements because Bapat et al. fails to disclose analogous

features. Thus, the rejection obfuscates the issue of anticipation by making broad references to sections of Bapat et al. without providing any guidance on the manner in which one is to interpret Bapat et al. as anticipating the claimed invention of the present application.

Applicant asserts that Bapat et al. completely fails to disclose any of the elements of claim 1, notwithstanding the references from the rejection into entire columns of text in Bapat et al.. Bapat et al. does not disclose the concept of a role filter, as recited within the first element of independent claim 1. Bapat et al. does not disclose the concept of associating a set of capabilities with a role, as recited within the second element of claim 1. Bapat et al. does not disclose the concept of a capability filter, as recited within the third element of claim 1. Bapat et al. does not disclose the concept of "authorizing access for a requesting principal to the protected resource based on an association between the requesting principal and the role and based on an association between the protected resource and a capability of the role", as recited within the fourth element of claim 1. Although the concept of a role or of role-based access within an access-control-based management model was well-known at the time of the present invention, as admitted in the background section of the present invention, Bapat et al. does not even disclose the use of roles, let alone a role filter as conceived with the present invention. Thus, although Bapat et al. clearly discloses an access-control-based management model, it is not clear whether the model that is disclosed within Bapat et al. can even be considered to disclose a role-based model.

In order to emphasize the fact that Bapat et al. does not disclose a role filter, capabilities associated with a role, and a capability filter, as required by the first three elements of independent claim 1, Applicant includes hereinbelow a copy of the

portion of Bapat et al. that was applied against the first elements of claim 1. As mentioned above, Bapat et al. also fails to disclose the features of the fourth element of claim 1. For the fourth element of claim 1, the rejection pointed to the entire text of columns 11 and 12 of Bapat et al.. Applicant could present a copy of that portion of Bapat et al. to emphasize that Bapat et al. does not disclose anything analogous to the fourth element of claim 1, but a simple referral to that portion of Bapat et al. should suffice; it is clear that Bapat et al. does not disclose the fourth element of claim 1. The text from column 9, line 45, to column 10, line 67, of Bapat et al., which was applied against the first three elements of claim 1 by the rejection, reads as follows:

The Access Control Database

While X.741 indicates that object access is to be controlled on a user by user basis, the present invention controls object access on a group by group basis. The user group feature helps to greatly reduce the amount of data required to define each access rule. Each user authorized to access information in the system is assigned to one or more groups. Access rules are defined in terms of access rights of groups. For instance, object parameter reading rights are likely to be assigned using different groups than object parameter setting rights. Also, rules are typically defined hierarchically with respect to these groups, for instance denying access to Customer A's subtree of objects to everyone who is not either a Customer A group member or a system administrator group member, and then further defining rights to objects within Customer A's subtree in accordance with groups of users set up by Customer A.

Referring to FIG. 4, the primary components of the access control tree 170 are group definitions 200, user definitions 202, target definitions 204, access rules 206, and default rules 208.

Each group definition 200 is represented by a group object, having the following fields:

group name; and

a list of users included in the group.

The group objects are used to map groups to users.

Each user definition 202 is represented by a user object, having the following fields:

user name; and

list of groups of which the user is a member.

The user objects are used to identify all the groups to which a particular user belongs.

It should be noted here that the term "users" includes entities other than users that can be granted access rights. For instance, the auxiliary servers, the log server, and even objects in the system can be set up as "users" for the purpose of defining access rights to be accorded to those entities.

Each target definition 204 is represented by a target object, having the following fields:

- target name; and

- a list of base managed objects that are to be included in the target set identified by this target object;

- a list of managed object classes; this field is used only when a target set includes all the managed objects of a particular class, subject to the filter condition (see below);

- scope, indicating the number of managed object tree levels below the listed base managed objects that are to be included in the target set; and

- a filter, which is an optional field used to restrict the set of objects included in the target set; the filter field is the equivalent of a "where" clause in a database query; and

- an operations list, which lists the operations (get, set, etc.) for which the target set is applicable.

Each rule definition 206 is represented by a rule object, having the following fields:

- a rule name for identifying the rule;

- a group list, that identifies all the user groups to which the rule is applicable;

- a targets list, which is a list of the target objects to which the rule is applicable; and

- an enforcement action, indicating whether the specified groups of users have or do not have access to the specified target set; in a preferred embodiment the enforcement action can be set to Deny with Response, Deny without Response, or Grant.

Default rules 208 are represented by a default rules object, having the following fields:

- a list of default enforcement actions for a corresponding predefined list of operations (e.g., get, set, create, delete, etc.); the most typical list of default enforcement actions is to deny access for all operations types, but in some implementations the system administrator might decide to make the default for some operations, such as the get operation, to be "grant";

- a default enforcement action for event notifications;
- and

a default denial response (i.e., deny with response or deny without response).

The defaults 208 are default responses that are defined for each operation when no rule has been defined that applies to a particular access request. For instance, the defaults could be set to "Grant" access requests whose operation is "Get", and to "Deny with Response" access requests whose operation is anything other than "Get". However, it is expected that in most implementations all the defaults will be set to either "Deny with Response" or "Deny without Response". The defaults 208 are preferably defined by a single Default object that contains a grant or deny flag for each of the defined operations.

Even though Bapat et al. fails to disclose various features of the present invention, it appears that Bapat et al. may have been chosen as a reference to be applied against the claims of the present application merely because Bapat et al. discloses the use of a type of filter within an access-control-based management model. Clearly, the filter that is disclosed in Bapat et al. is not a role filter nor a capability filter. It should not need mentioning that mere term matching is not a proper foundation for an anticipation argument in a rejection of patent claims.

With respect to dependent claims 2-10, Bapat et al. does not disclose, at a minimum, the subject matter in independent claim 1 from which these dependent claims depend. Thus, Bapat et al. also fails to disclose the features of the dependent claims because these dependent claims include the features of independent claim 1.

Moreover, the dependent claims recite additional elements, and these elements also fail to be disclosed in Bapat et al.. In fact, the rejections of dependent claims 2-10 are as non-specific as the rejection of independent claim 1 from which they depend. For example, columns 11-12 are applied against claim 3; columns 16-18 are applied against claim 5; "Figure 9 and associated text" is applied against claim 6; "Figure 5 and associated text" is applied against claim 7; columns 24-25 are applied against claim 8; and columns 8-9 are applied against claim 10. Again, the lack

of detail in the rejections mirror the lack of disclosure in Bapat et al.. The rejections of claim 2, 4, and 9 are slightly more specific as they reference ten to thirty lines of text within Bapat et al., but because each of these claims contains some feature relating to a role filter or a capability filter, and Bapat et al. fails to disclose a role filter or a capability filter, these portions of Bapat et al. appear to have been selected at random because there is no argument as why these portion of Bapat et al. seem to be relevant in any manner whatsoever. The features in the dependent claims are also clearly absent from Bapat et al., notwithstanding the argument in the rejections.

Claims 1-10 are directed to a method; claims 11-20 are directed to an apparatus; and claims 21-30 are directed to a computer program product. The Office action uses an anticipation argument against claims 11-30 by relying the argument that is used against claims 1-10. Applicant's arguments with respect to the rejection of claims 1-10 are similarly applicable against the rejection of claims 11-30.

Bapat et al. clearly does not disclose features as required by the language of the claims of the present application. As stated at MPEP § 2131: "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). "The identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). Hence, Bapat et al. cannot be used as an anticipatory reference, and the rejection of claims 1-30 has been overcome, whereby Applicant requests the withdrawal of the rejection.

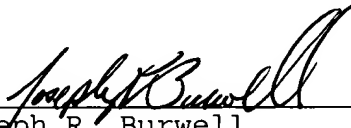
IV. Conclusion

It is respectfully urged that the present patent application is patentable, and Applicant kindly requests a Notice of Allowance.

For any other outstanding matters or issues, the examiner is urged to call or fax the below-listed telephone numbers to expedite the prosecution and examination of this application.

DATE: August 18, 2004

Respectfully submitted,



Joseph R. Burwell
Reg. No. 44,468
ATTORNEY FOR APPLICANT

Law Office of Joseph R. Burwell
P.O. Box 28022
Austin, Texas 78755-8022
Voice: 866-728-3688 (866-PATENT8)
Fax: 866-728-3680 (866-PATENT0)
Email: joe@burwell.biz